UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

ALEJANDRO MONROY, on behalf of himself and all others similarly situated,

Plaintiff,

v.

SHUTTERFLY, INC.,

Defendant.

Civil Action No.: 16-cv-10984

Hon. Joan B. Gottschall

Magistrate Judge Jeffrey T. Gilbert

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS

Lauren R. Goldman
Michael Rayfield*
MAYER BROWN LLP
1221 Avenue of the Americas
New York, NY 10020
Telephone: (212) 506-2500
lrgoldman@mayerbrown.com
mrayfield@mayerbrown.com

John Nadolenco (*pro hac vice*)
MAYER BROWN LLP
350 South Grand Avenue
25th Floor
Los Angeles, CA 90071
Telephone: (213) 229-9500
jnadolenco@mayerbrown.com

**pro hac vice* motion forthcoming

Counsel for Defendant Shutterfly, Inc.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

INTRODUCTION

Shutterfly is a manufacturer and digital retailer of personalized products and services. Its services include free online tools that allow people to upload, organize, and share digital photographs in a centralized, easily accessible location. Users of these tools can "tag" photos with information—such as names—to make them easier to organize and share. To facilitate this process, Shutterfly uses facial-recognition technology to analyze uploaded photos, and then employs information derived from that analysis to suggest potential tags to users.

Plaintiff challenges this helpful feature by invoking an Illinois statute that has no connection either to him or to the technology at issue. Plaintiff does not use Shutterfly and he does not live in Illinois, but he alleges that an unidentified Shutterfly user in Illinois tagged a photo with his name, and that Shutterfly then used facial-recognition technology to extract "biometric data" from this photo. Plaintiff claims that this violated the Illinois Biometric Information Privacy Act (BIPA), a statute enacted in 2008 to regulate the use of biometric technologies (like retina scans and fingerprints) in connection with financial transactions and security screenings (not photo-tagging features) occurring in this State.

The complaint should be dismissed for three independently sufficient reasons, all of which reflect the utter disconnect between plaintiff's allegations and the BIPA statute. First, BIPA applies only to "biometric identifiers" and "biometric information." The statute expressly defines those terms to *exclude* "photographs" and any "information derived from" photographs. Because plaintiff's claim is based entirely on Shutterfly's alleged extraction of information from photographs, it fails under BIPA's plain terms.

Second, BIPA does not apply to the out-of-state conduct alleged here, both (a) because the statute does not apply extraterritorially and (b) because the dormant Commerce Clause precludes Illinois from imposing its legislative decisions on other states that have chosen not to enact similar laws. Plaintiff is a resident of Florida, Shutterfly is headquartered in California, and plaintiff does not allege that Shutterfly analyzed his photo or stored the resulting data in Illinois. The sole Illinois connection alleged by plaintiff—that the photograph was uploaded by a Shutterfly user at a time when he or she was located in Illinois—has no relevance to the purpose of BIPA or the conduct that it regulates. Under plaintiff's theory, BIPA imposes obligations on the out-of-state collection of biometric data from out-of-state individuals. Neither Illinois law nor the Constitution permits that result.

Finally, BIPA allows a plaintiff to recover only if he has suffered "actual damages." Plaintiff does not, and cannot, allege that he has suffered such damages. Two courts—one state and one federal—have held that such allegations are required; this Court should do the same.

BACKGROUND

A. The Illinois Biometric Information Privacy Act

BIPA was enacted in 2008 to address the growing use of biometric data "in the *business and security screening sectors*" in Illinois. 740 ILCS 14/5(a) (emphasis added). The Illinois General Assembly found that "[m]ajor national corporations ha[d] selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." *Id.* 14/5(b). Consumers had become wary "of the use of biometrics when such information is tied to finances" and were being "deterred from partaking in biometric identifier-facilitated transactions," in part because of the "limited State law regulating the collection, use, safeguarding, and storage of biometrics." *Id.* 14/5(d), (e).

BIPA addresses these concerns by regulating the collection and storage of (1) "biometric identifiers" and (2) "biometric information." The statute defines "biometric identifier" using a short, exclusive list of sources of data about a person: "'Biometric identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." *Id.* 14/10. Other potential identifiers are then expressly excluded from the definition: "Biometric identifiers do not include writing samples, written signatures, *photographs*, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color." *Id.* (emphasis added).

"Biometric information" is data derived from a biometric identifier: "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id.* This provision, too, contains an exclusionary clause: "Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers"—such as "photographs." *Id.* Thus, both "photographs" and "information derived from" photographs are removed from BIPA's coverage.

BIPA requires private entities that "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information" to first (1) inform the person of that collection or storage "in writing"; (2) inform the person "in writing of the specific purpose and length of term" of the collection, storage, and usage; and (3) obtain a "written release" from the person. *Id.* 14/15(b). Private entities are also required to develop and publish a written policy regarding the retention and destruction of biometric data. *Id*. 14/15(a).

For intentional or reckless violations of BIPA, a plaintiff can collect "liquidated damages of $5,000 or actual damages, whichever is greater"; for negligent violations, the plaintiff can obtain "liquidated damages of $1,000 or actual damages, whichever is greater." *Id.* 14/20.

B. Prior BIPA Lawsuit Against Shutterfly

In June 2015, a different plaintiff represented by the same counsel filed a similar BIPA lawsuit against Shutterfly in this District. *See Norberg v. Shutterfly, Inc.*, No. 15-cv-05351 (N.D. Ill. 2015). Judge Norgle denied Shutterfly's motion to dismiss. *Norberg v. Shutterfly, Inc.*, 152

F. Supp. 3d 1103 (N.D. Ill. Dec. 29, 2015). Shutterfly then filed a motion to compel arbitration based on public information indicating that the photo at issue had been uploaded by the plaintiff's wife, a Shutterfly user bound by an arbitration clause. *See Norberg* Dkt. 79. The case settled three weeks later and was dismissed with prejudice. *See Norberg* Dkts. 89, 91.

C. Plaintiff's Claim

Evidently unable to find another Illinois resident willing to sue Shutterfly under BIPA, plaintiff's counsel filed this suit on behalf of Florida resident Alejandro Monroy seven months later, on November 30, 2016. The complaint alleges that Shutterfly uses facial-recognition software to "extract[], collect[], and store[] millions of 'scans of face geometry'—highly detailed geometric maps of the face—from every individual who appears in a photograph uploaded to Shutterfly, including non-users." Compl. (Dkt. 1) ¶ 5. Plaintiff asserts that Shutterfly uses this information to suggest tags for faces in uploaded photographs that match "scans of face geometry already saved in Shutterfly's face database," and that these "scans" are "biometric identifiers" covered by BIPA. *Id.* ¶¶ 19, 21, 22, 23. He claims that "[t]hese unique biometric identifiers are not only collected and used by Shutterfly to identify individuals by name, but also to recognize their gender, age, race and location"; and that "[a]ccordingly, Shutterfly also collects 'biometric information' from individuals appearing in user-uploaded photos." *Id.* ¶ 24.

Plaintiff is neither a resident of Illinois nor "a Shutterfly user"; he "has never used Shutterfly's services in any way." *Id.* ¶¶ 1, 7, 27. He claims that in 2014, a Shutterfly user in Chicago uploaded a photograph of him,[1] and that Shutterfly then analyzed this photo using facial-recognition technology without complying with BIPA's notice and consent provisions. *Id.*

[1] Shutterfly's Terms of Use prohibit users from "[u]pload[ing] photographs of people who have not given permission for their photographs to be uploaded to a share site." Terms of Use, Shutterfly, http://shutterflyinc.com/terms.html.

¶¶ 28-35. Plaintiff seeks to represent a putative class of "[a]ll individuals who are not users of Shutterfly and who had their biometric identifier, including scan of face geometry, collected, captured, received, or otherwise obtained by Shutterfly from a photograph uploaded to Shutterfly's website from within the state of Illinois." *Id.* ¶ 36.

ARGUMENT[2]

I. BIPA DOES NOT APPLY TO SHUTTERFLY'S TECHNOLOGY.

Plaintiff's claim fails because BIPA's plain language expressly excludes both photographs and information derived from them. BIPA's legislative findings and history confirm that these broad exclusions were intentional.

A. BIPA's Plain Language Expressly Excludes "Photographs" And Any "Information Derived From" Photographs.

Plaintiff repeatedly and consistently recognizes that his case rests entirely on *photographs* that people voluntarily upload to Shutterfly. Compl. ¶¶ 4-5, 18, 22-23, 25, 28-31, 44. This dooms his claim: BIPA's definition of "biometric identifier" excludes "photographs," and its definition of "biometric information" excludes "information derived from items or procedures excluded under the definition of biometric identifiers"—such as photographs. 740 ILCS 14/10. Under BIPA's plain terms, that should end the discussion.

Remarkably, the complaint makes *no mention* of these exclusions. Instead, plaintiff relies solely on the term "scan of . . . face geometry" in the definition of "biometric identifier." *Id*. He alleges that this term covers the "highly detailed geographic maps of the face" that Shutterfly allegedly "has extracted, collected and stored . . . from . . . photographs[s] uploaded to Shutterfly." Compl. ¶¶ 5, 22; *see id.* ¶¶ 10, 23, 30-33, 36, 44. That is wrong for two reasons.

[2] "A motion to dismiss should be granted if the plaintiff fails to offer 'enough facts to state a claim to relief that is plausible on its face.'" *Ennenga v. Starns*, 2012 WL 1899331, at *2 (N.D. Ill. May 23, 2012) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007)).

First, plaintiff's approach ignores the structure of the statute. In enacting BIPA, the legislature created two categories of covered biometric data: (1) original sources of information about a person ("biometric identifiers"—defined as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry"); and (2) data extracted or derived from those sources ("biometric information"—defined as "information . . . based on an individual's biometric identifier"). If data "extracted" from "photograph[s]" (Compl. ¶ 5) were covered by BIPA, it would be regulated within the category of "biometric information." But that is plainly not the case—a photograph is one of the "items or procedures" excluded from the meaning of "biometric identifier," and accordingly "information derived from" photographs is excluded from the definition of "biometric information." 740 ILCS 14/10. There can be no question that the legislature went out of its way to exclude, across the board, *both* photographs and information derived from photographs. That effort would be meaningless if information derived from photographs were somehow jammed into the definition of "biometric identifier."

Second, even taking the enumerated list of "biometric identifiers" in isolation (and ignoring the express exclusions), Shutterfly's technology does not involve a "scan of . . . face geometry." Under a "commonsense canon" of construction, the meaning of this term is "narrowed by . . . the neighboring words with which it is associated," *United States v. Williams*, 553 U.S. 285, 294 (2008), in order "to avoid ascribing to one [term] a meaning so broad that it is inconsistent with its accompanying words," *People v. Qualls*, 365 Ill. App. 3d 1015, 1020 (2006). In BIPA, the term "scan of . . . face geometry" means an *in-person* scan of a person's *actual* face—not the application of facial-recognition software to a photograph.

The terms surrounding "scan of . . . face geometry" all describe physical, in-person processes for obtaining information about an individual that can be used to authenticate a transaction or access a secure area. A "retina scan" involves a live person holding his eye to a specialized machine.[3] A "fingerprint" is produced when a live person touches a card, console, or other object.[4] A "voiceprint" is the product of a live person's spoken words.[5] And most notably, a "scan of hand geometry"—the statutory term closest to "scan of face geometry"—can be accomplished *only* in person: A person's actual hand "is placed on [a] plate, palm down, and guided by five pegs that sense when the hand is in place," and then a camera "capture[s] a silhouette image of the hand."[6] Similarly, a "scan of face geometry" requires a person to present his actual face at a console or other scanner, such as those widely used at airports.

Shutterfly, by contrast, does not use a specialized device to conduct a live capture of a person's actual face. Instead, a person takes an ordinary picture and then (at some point later) he might voluntarily upload it to Shutterfly. On plaintiff's theory, Shutterfly was required to give notice to, and obtain consent from, *non-users* with whom it has *never interacted*—people it cannot even identify or contact. That is implausible: BIPA does not require services like Shutterfly to obtain consent from every person in the world who might appear in a photo.

[3] *See* Rawlson King, *Explainer: Retinal Scan Technology*, BiometricUpdate.com (July 12, 2013), http://www.biometricupdate.com/201307/explainer-retinal-scan-technology ("A retinal scan is performed by casting an unperceived beam of low-energy infrared light into a person's eye as they look through the scanner's eyepiece.").

[4] *See* FBI, *Recording Legible Fingerprints*, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/recording-legible-fingerprints ("[f]ingerprints can be recorded" either with ink on a "standard fingerprint card" or "electronically using a *live* scan device" (emphasis added)).

[5] *See* Lisa Myers, *An Explanation of Voice Biometrics*, SANS Institute, at 4 (July 24, 2004), https://www.sans.org/reading-room/whitepapers/authentication/exploration-voicebiometrics-1436 ("[t]he user is asked to speak a certain set of words or phrases, or to speak for a certain length of time," and "[f]rom that sample, a digital representation of the voice, called a voiceprint, is created").

[6] Stephen Mayhew, *Explainer: Hand Geometry Recognition*, BiometricUpdate.com (June 22, 2012), https://www.biometricupdate.com/201206/explainer-hand-geometry-recognition.

B. BIPA's Legislative Findings and History Confirm That The Statute Was Not Intended To Regulate Data Derived From Online Photographs.

The General Assembly's findings confirm that it *deliberately* excluded photos and information derived from them. BIPA was designed to regulate the live use of biometric technologies in connection with "financial transactions and security screenings," 740 ILCS 14/5(a)—not the application of facial-recognition software to photographs. The legislature believed that the increasing use of "biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias," would have a "streamlin[ing] effect" on Illinois commerce. 740 ILCS 14/5(a), (b). But it anticipated that the "limited State law" in this area would create identity-theft concerns, "deterr[ing] [consumers] from partaking in biometric identifier-facilitated transactions" and perhaps causing them to "withdraw" from such "transactions" altogether. *Id.* 14/5(c), (e).

The legislative history confirms BIPA's limited purpose. As BIPA moved toward passage, the definitions of "biometric identifier" and "biometric information" were sharply narrowed. The first Senate version defined "biometric identifier" broadly: "Examples of biometric identifiers *include, but are not limited to*[,] iris or retinal scans, fingerprints, voiceprints, and *records* of hand or facial geometry." Sen. Bill 2400, § 10 (Feb. 14, 2008) (Ex. A) (emphases added). And although the definition of "biometric identifier" always excluded "photographs," the original definition of "biometric information" did not exclude information derived from photographs. *Id.* The next proposal was even broader: "biometric identifier" included "records or scans of hand geometry, facial geometry, or *facial recognition*." Sen. Am. to Sen. Bill 2400, § 10 (Apr. 11, 2008) (Ex. B) (emphasis added). But that proposal was rejected, and the House offered a version that was substantially narrower than the original: it (a) changed the definition of "biometric identifiers" from an open-ended set of "[e]xamples" to a narrow list of enumerated sources; (b) removed the broad term "records" of hand or face geometry; and (c) excluded from the definition of "biometric information" all "information derived from items or procedures excluded under the definition of biometric identifiers." House Am. to Sen. Bill 2400, § 10 (May 28, 2008) (Ex. C). The statute was enacted with these changes.

In sum, consistent with its findings, the legislature expressly *declined* to include a "record" of facial geometry in the definition of biometric identifier; to regulate all forms of "facial recognition"; or to allow information derived from photographs to slip into the definition of "biometric information." Plaintiff's theory cannot be squared with these policy decisions.

C. The Court Should Not Follow *Norberg* Or *Facebook Biometric*.

Two decisions have denied motions to dismiss BIPA claims based on the application of facial-recognition technology to photos: *Norberg v. Shutterfly*, *supra*, and *In re Facebook Biometric Information Privacy Litigation*, 185 F. Supp. 3d 1155 (N.D. Cal. 2016). Shutterfly respectfully submits that each of these cases was wrongly decided.

In *Norberg*, the court's substantive analysis of BIPA was limited to a paragraph:

> Here, Plaintiff alleges that Defendants are using his personal face pattern to recognize and identify Plaintiff in photographs posted to Websites. Plaintiff avers that he is not now nor has even been a user of [the] Websites, and that he was not presented with a written biometrics policy nor has he consented to have his biometric identifiers used by Defendants. As a result, the Court finds that Plaintiff has plausibly stated a claim for relief under the BIPA.

152 F. Supp. 3d at 1106. The court did not even attempt to square the operation of Shutterfly's technology with BIPA's exclusion of photographs and information derived from them.

In *Facebook Biometric*, a California federal court held that BIPA covers "newer technology like scans of face geometry" and expressly excludes *only* "physical identifiers that are more qualitative and non-digital in nature." 185 F. Supp. 3d at 1171. Accordingly, the court concluded that "'[p]hotographs' is better understood to mean *paper prints* of photographs, not digitized images stored as a computer file and uploaded to the Internet." *Id.* (emphasis added). This reading cannot be reconciled with the technologies covered as "biometric identifiers": Fingerprints are hardly a "newer technology" and are often "physical" and "non-digital"; and hand, retina, and iris scans have existed for decades. 740 ILCS 14/10; King, *supra* n.3. Nor can the court's reading be reconciled with the commonly understood meaning of "photograph" when the statute was passed in 2008: by then, digital photography was already the norm. The legislature was not distinguishing between newer and older technologies; it was seeking to regulate sources of data that presented particular policy concerns, and it decided that *photographs and information derived from them* did not present those issues. *See* pp. 2, 8 *supra*.

II. BIPA DOES NOT AND CANNOT REGULATE OUT-OF-STATE CONDUCT.

Setting aside whether the General Assembly intended to regulate Shutterfly's technology, plaintiff's claim fails because Illinois has no interest in this suit. BIPA does not apply to alleged violations occurring outside of the State, and any such application would be unconstitutional.

A. Plaintiff Has Not Alleged A Sufficient Nexus To Illinois For BIPA To Apply.

Illinois has a "long-standing rule of construction" that a "statute is without extraterritorial effect unless a clear intent in this respect appears from the express provisions of the statute." *Avery v. State Farm Mut. Auto. Ins. Co.*, 216 Ill. 2d 100, 184-85 (2005). Nothing in BIPA conveys any such intent. To be actionable, then, a BIPA violation must occur *within* Illinois.

Avery held that "a transaction may be said to take place within a state if the circumstances relating to the transaction occur *primarily and substantially* within that state." 216 Ill. 2d at 186 (emphasis added). Put differently, "the *majority of circumstances* relating to the alleged *violation of the [statute]*" must have occurred in the state. *Landau v. CNA Fin. Corp.*, 381 Ill. App. 3d 61, 65 (2008) (emphases added). Here, plaintiff does not allege that *any* significant circumstance occurred in Illinois. Shutterfly is a Delaware corporation headquartered in California, and plaintiff is a resident and citizen of Florida. Compl. ¶¶ 7-8. Plaintiff has never interacted with Shutterfly in Illinois (or anywhere else). *Id.* ¶ 27. Plaintiff does not allege that Shutterfly analyzed his photo or stored the resulting data—the only "violation of the [statute]" alleged—in Illinois. Nor does plaintiff claim that he suffered injury in Illinois.[7]

Plaintiff claims only one connection to Illinois: that his photo was uploaded to Shutterfly (by an unidentified non-party who is not even alleged to be an Illinois resident) from a device that was "physically located within the state." *Id.* ¶ 28. That slim reed is not nearly enough to support the application of Illinois law. Indeed, Illinois courts have held that even when "a *scheme to defraud* was disseminated from a *[defendant's] headquarters in Illinois*," that fact alone "is insufficient" to trigger Illinois law if "'the overwhelming majority of circumstances' pertaining to [a plaintiff's] claims took place outside Illinois." *Philips v. Bally Total Fitness Holding Corp.*, 372 Ill. App. 3d 53, 58-59 (2007) (emphases added) (quoting *Avery*, 216 Ill. 2d at 188). It therefore cannot be sufficient, standing alone, that a *non-party's* indisputably *innocent* conduct (the upload of a photograph) allegedly took place in this State.

BIPA's purpose confirms this point: it was enacted because "[m]ajor national corporations ha[d] selected . . . *locations in this State as pilot testing sites* for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores,

[7] *See Avery*, 216 Ill. 2d at 188 (no in-state transaction where, among other things, plaintiff was not an Illinois resident and there was "no evidence that [plaintiff] ever met or talked to a State Farm employee who works in Illinois"); *Int'l Profit Assocs., Inc. v. Linus Alarm Corp.*, 361 Ill. Dec. 661, 672 (App. Ct. 2012) ("[G]iven that the alleged deception and injury took place in Florida, the majority of relevant facts . . . cannot be said to have taken place primarily and substantially in Illinois."); *Landau*, 381 Ill. App. 3d at 64-65 (Illinois statute did not apply where plaintiff did not reside in Illinois; his "contact with company representatives occurred only in Pennsylvania"; and the "violation of the" statute took place outside Illinois); *Haught v. Motorola Mobility, Inc.*, 2012 WL 3643831, at *3 (N.D. Ill. Aug. 23, 2012) (factors under *Avery* include "claimant's residence" and "defendant's place of business"); *Valley Air Serv. v. Southaire, Inc.*, 2009 WL 1033556, at *12 (N.D. Ill. Apr. 16, 2009) (Illinois statute did not apply where alleged "wrongful activity" occurred outside of state).

gas stations, and school cafeterias." 740 ILCS 14/5(b) (emphasis added). The bill's chief sponsor said that regulating such transactions was "especially important" because "the largest fingerprint scan system *in Illinois* [] ha[d] recently filed for bankruptcy," "leav[ing] thousands of customers" of stores in Illinois "wondering what will become of their biometric and financial data." IL H.R. Tran. 2008 Reg. Sess. No. 276, at 249 (May 30, 2008) (Ex. D) (emphasis added). BIPA addresses in-state transactions in which the consumer's "biometric[] . . . information is tied to [his] finances," 740 ILCS 14/5(d); it was never intended to regulate a California corporation's application of facial-recognition software to a photo of a Florida resident.

B. If Applied Here, BIPA Would Violate The Dormant Commerce Clause.

Like the extraterroriality doctrine, the U.S. Constitution ensures that a state regulates only conduct that it has a substantial interest in controlling. Article I, section 8 gives Congress the exclusive power to regulate commerce "among the several states." This express grant of power implicitly "limit[s] . . . the authority of the States to enact legislation affecting interstate commerce." *Healy v. Beer Inst., Inc.*, 491 U.S. 324, 326 n.1 (1989). The "dormant Commerce Clause" "precludes the application of a state statute" that has "the practical effect of . . . control[ling] conduct beyond the boundaries of the State," "whether or not the commerce has effects within the State"—thereby preventing "inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State." *Id.* at 336-37.

On plaintiff's theory, if a Californian took a vacation in Miami, snapped a photo of a Florida resident, then uploaded the photo to Shutterfly during a layover at O'Hare on his way home, and Shutterfly then analyzed that photo from its California headquarters, Shutterfly would have to comply with this Illinois statute by informing the Floridian in the photo and obtaining a "written release." 740 ILCS 14/15(b). Illinois has no interest in regulating this set of facts.

And Illinois certainly does not have a sufficiently strong interest to *displace* the inconsistent policies of California and Florida. In applying the dormant Commerce Clause, the Seventh Circuit has "t[aken] a broad[] view" of what constitutes an inconsistent legal regime. *Midwest Title Loans, Inc. v. Mills*, 593 F.3d 660, 667-68 (7th Cir. 2010). A showing of "inconsistent *obligations*" is not required; "the *absence* of a . . . counterpart" law in another state generally demonstrates that the other state "thinks [the conduct] shouldn't be restricted in the [same] way," and it would be unconstitutional to "exalt the public policy of one state over that of another." *Id.* (emphases added); *see Morrison v. YTB Int'l, Inc.*, 649 F.3d 533, 538 (7th Cir. 2011) ("Some states allow gambling; others don't. Some allow fireworks; others don't. Perhaps some allow pyramid schemes. Expanding Illinois law in a way that overrode the domestic policy of other states would be problematic."); *Morley-Murphy Co. v. Zenith Elecs. Corp.*, 142 F.3d 373, 379 (7th Cir. 1998) (absent dormant Commerce Clause, "any state that has chosen a policy more *laissez faire* than Wisconsin's would have its choices stymied, because the state that has chosen more regulation could always trump its deregulated neighbor"). No state with a real connection to this lawsuit has chosen to pass a statute regulating facial-recognition technology. California (Shutterfly's home state) has at least once *considered and rejected* such a law. Cal. Sen. Bill No. 169 (July 5, 2001) (Ex. E) (law that would regulate "facial recognition technology," defined as "the use of a facial image in combination with a system to record and translate facial features, or the spatial relationship between facial features, into a unique numerical template"). Nor has Florida (plaintiff's home) passed such a statute. The Commerce Clause precludes Illinois from overriding these states' decisions to stay out of the field.

This principle is particularly important in the Internet context. "[C]ourts have long recognized that certain types of commerce demand consistent treatment," and that "[t]he Internet represents one of those areas": "Regulation by any single state can only result in chaos, because at least some states will likely enact laws subjecting Internet users to conflicting obligations." *Am. Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 181 (S.D.N.Y. 1997); *see also Am. Booksellers Found. v. Dean*, 342 F.3d 96, 104 (2d Cir. 2003) ("the internet will soon be seen as falling within the class of subjects that are protected from State regulation" under dormant Commerce Clause); *ACLU v. Johnson*, 194 F.3d 1149, 1162 (10th Cir. 1999). At the very least, the "massive liability brought on by conflicting applicable law could chill . . . the rapidly expanding field of Internet commerce." *Archdiocese of St. Louis v. Internet Entm't Grp., Inc.*, 1999 WL 66022, at *3 (E.D. Mo. Feb. 12, 1999). At worst, these "inconsistent regulatory schemes could paralyze the development of the Internet altogether." *Pataki*, 969 F. Supp. at 181.

III. PLAINTIFF HAS NOT ALLEGED ACTUAL DAMAGES AND THEREFORE CANNOT RECOVER STATUTORY DAMAGES UNDER BIPA.

At a minimum, the Court should dismiss plaintiff's claim for statutory damages. BIPA allows a party to collect only "liquidated damages"—of either $1,000 or $5,000, depending on the willfulness of the violation—"or actual damages, whichever is greater." 740 ILCS 14/20(1)-(2). Under controlling precedent, this kind of liquidated damages provision applies only when the plaintiff can prove that he *suffered* actual damages but cannot prove their full *amount*. Here, plaintiff does not even *seek* actual damages, let alone allege that he suffered them. *Cf.* Compl. ¶ 52 (seeking only injunctive relief, statutory damages, fees, and costs).

In *Sterk v. Redbox Automated Retail, LLC*, 672 F.3d 535 (7th Cir. 2012), the Seventh Circuit addressed a federal statute that allowed private parties to collect "actual damages but not less than liquidated damages in an amount of $2,500." *Id.* at 537. The Court of Appeals recognized that this provision did not *expressly* require a plaintiff to prove actual damages in order to collect liquidated damages, but concluded that this was the only "sens[ible]" reading of the statute: "True, [the provision] allows $2,500 in 'liquidated damages,' without need to prove 'actual damages,' but liquidated damages are intended to be an estimate of actual damages, and if [the statutory violation] results in no injury at all . . . , the only possible estimate of actual damages . . . would be zero." *Id.* at 538 (citation omitted); *see also Pace Commc'ns, Inc. v. Moonlight Design, Inc.*, 31 F.3d 587, 593 (7th Cir. 1994) (a liquidated damages "provision must be a reasonable attempt to estimate actual damages"). *Sterk* relied upon *Doe v. Chao*, 540 U.S. 614 (2004), which addressed a statute providing that a plaintiff could collect "actual damages sustained . . . as a result of [a violation], but in no case [could] a person entitled to recovery receive less than the sum of $1,000." *Id.* at 619. The Supreme Court held that the plaintiff was not entitled to a statutory award because he had failed to prove actual damages: "the statute d[id] not speak of liability (and consequent entitlement to recovery) in a freestanding, unqualified way, but in a limited way, by reference to enumerated damages." *Id.* at 620-21.

The same is true of BIPA. If a plaintiff has suffered actual damages, he may collect the *greater* of those damages or the specified amount of liquidated damages. But BIPA does not permit recovery where (as here) no actual damages have been suffered or even alleged. *See McCollough v. Smarte Carte, Inc.*, 2016 WL 4077108, at *4 (N.D. Ill. Aug. 1, 2016) (explaining "the need for proof of an actual injury to recover[] statutory damages like those provided in BIPA" (citing *Doe* and *Sterk*)); Hr'g Tr. at 55, *Rottner v. Palm Beach Tan, Inc.*, No. 2015-CH-16695 (Ill. Cir. Ct. Dec. 20, 2016) (Ex. F) ("[P]laintiff [could not] plead actual damages or entitlement to liquidated damages without any reasonable or plausible showing of harm or actual damages resulting from the alleged BIPA violation."). An award of liquidated damages would not be a "reasonable attempt to estimate actual damages," but rather a "penalty clause[]" of the kind that "Illinois courts" have "refus[ed] to enforce." *Pace*, 31 F.3d at 593.

CONCLUSION

The Court should dismiss the complaint with prejudice.

Date: February 6, 2017

By: /s/ *Lauren R. Goldman*

Lauren R. Goldman
Michael Rayfield*
MAYER BROWN LLP
1221 Avenue of the Americas
New York, NY 10020
Telephone: (212) 506-2500
lrgoldman@mayerbrown.com
mrayfield@mayerbrown.com

John Nadolenco (*pro hac vice*)
MAYER BROWN LLP
350 South Grand Avenue
25th Floor
Los Angeles, CA 90071
Telephone: (213) 229-9500
jnadolenco@mayerbrown.com

**pro hac vice* motion forthcoming

Counsel for Defendant Shutterfly, Inc.